Introduction to Identity and Access Management (IAM)

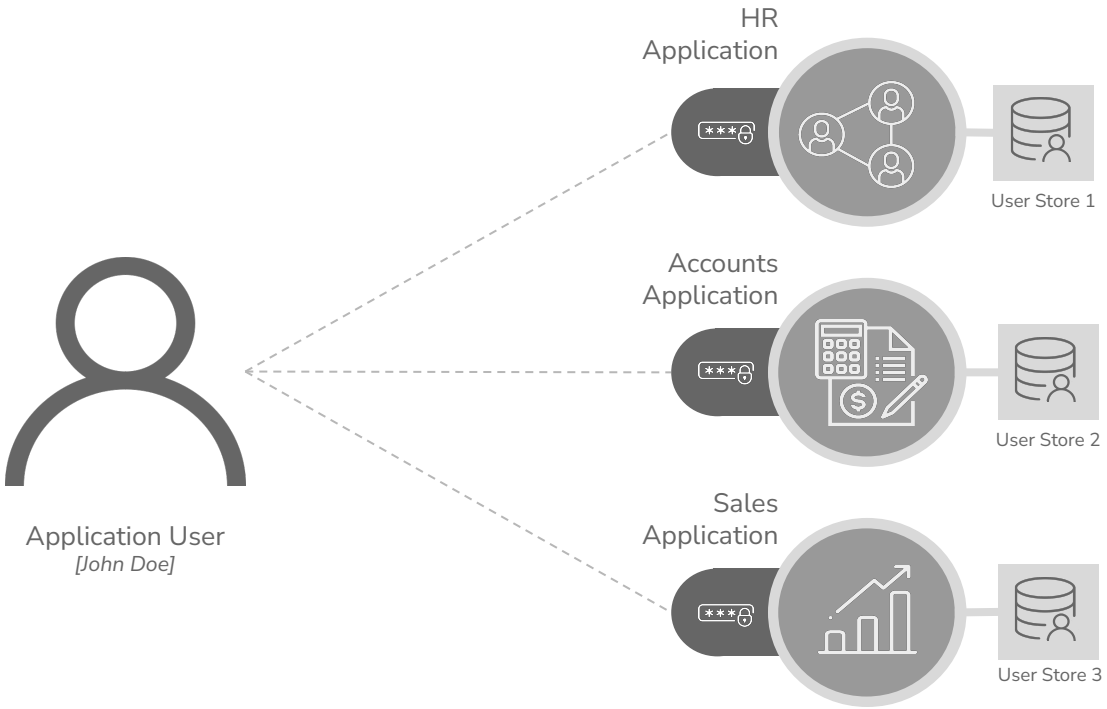
Why Identity and Access Management (IAM)?

- Securely store and manage user identities and access privileges
- Ensure user identity and grant access to the **right resources** at the **right time** for the **right reasons**
- Provide a better user experience (UX)
- Enable regulatory and privacy compliances
- Increases productivity and reduce IT costs
- Get your app to market faster

Traditional Access Management

Managing access at the application level

In traditional web app login, authentication and account management happens within each individual application



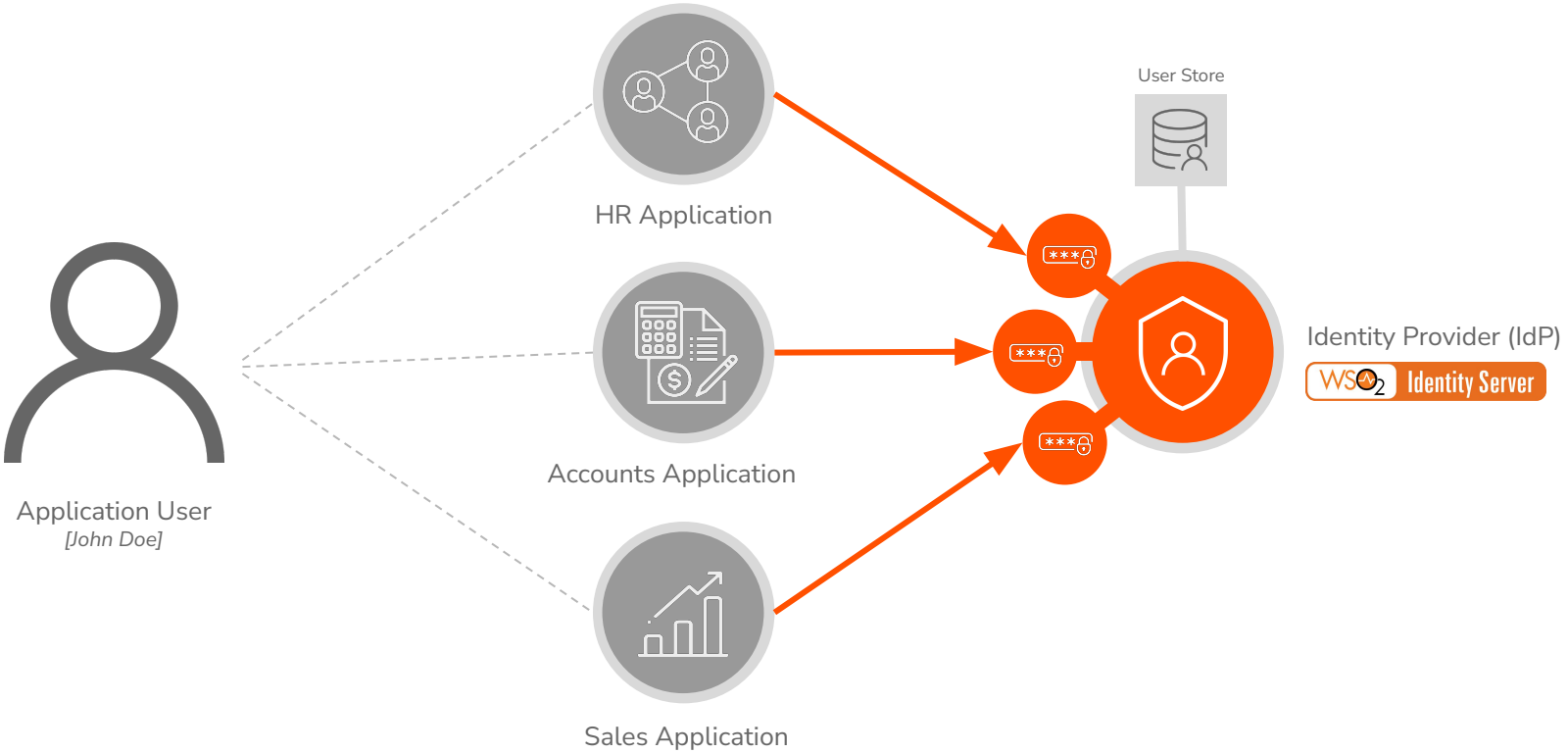
Issues with Traditional Access Management

- Higher chances of data breaching
  - Using simple passwords or same password for multiple applications
  - Security and account management is not a cornerstone in applications
- Minimum UX
  - Remembering multiple login credentials is a hassle
  - Login experiences might not be consistent
  - Having to wait till the admin team create accounts for each application
- Difficulty in governance
- Less agility and low productivity
- High IT cost
- Difficulty in complying to regulations

Identity and Access Management Concepts

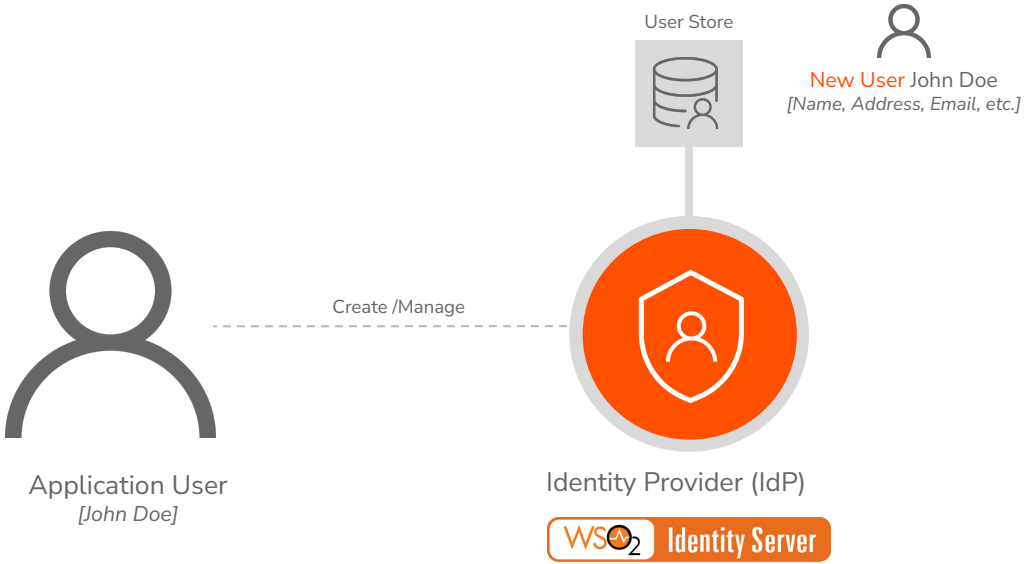
Centralized Access Management

A central system handles user authentication and account management



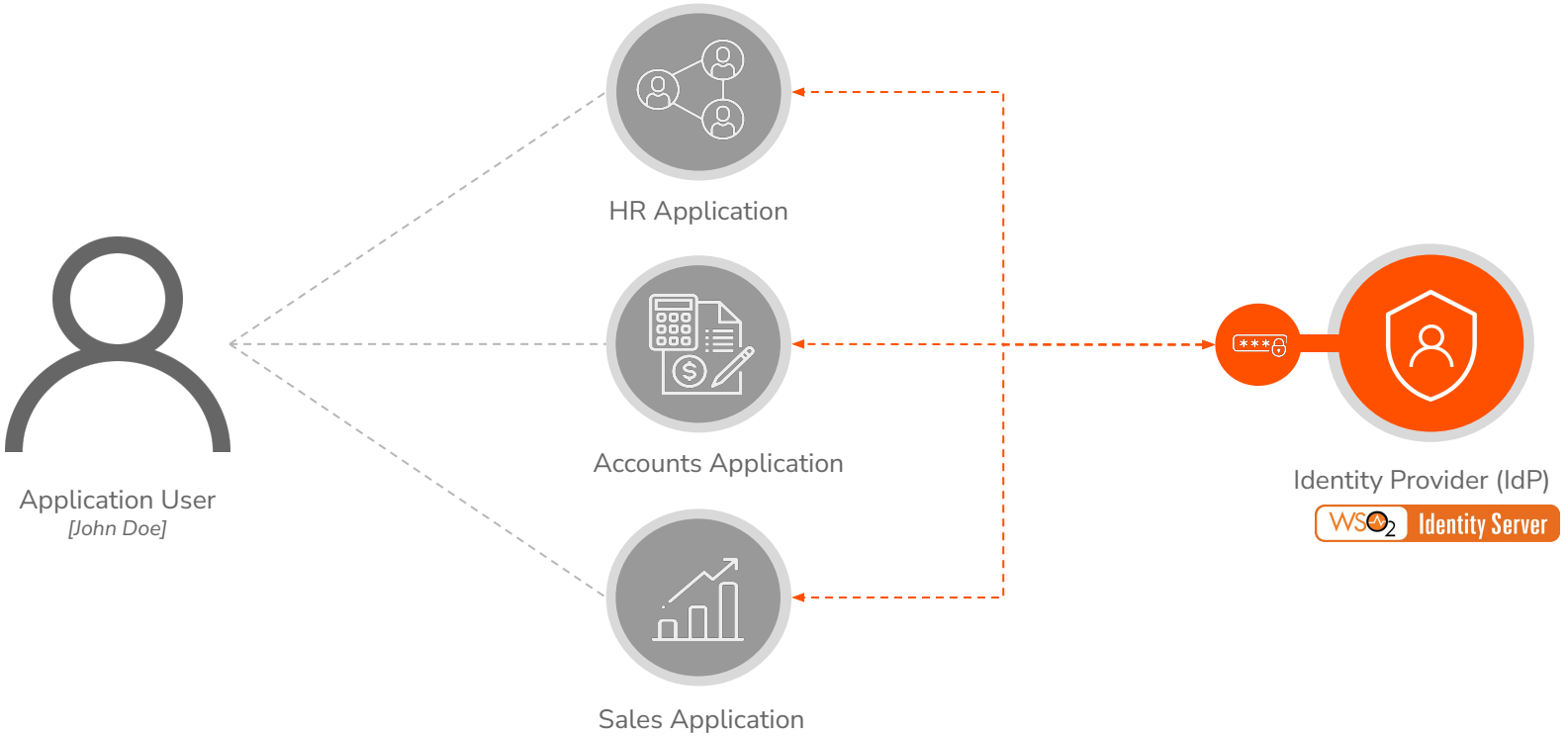
User Provisioning

Process of creating and managing user accounts and information within the system



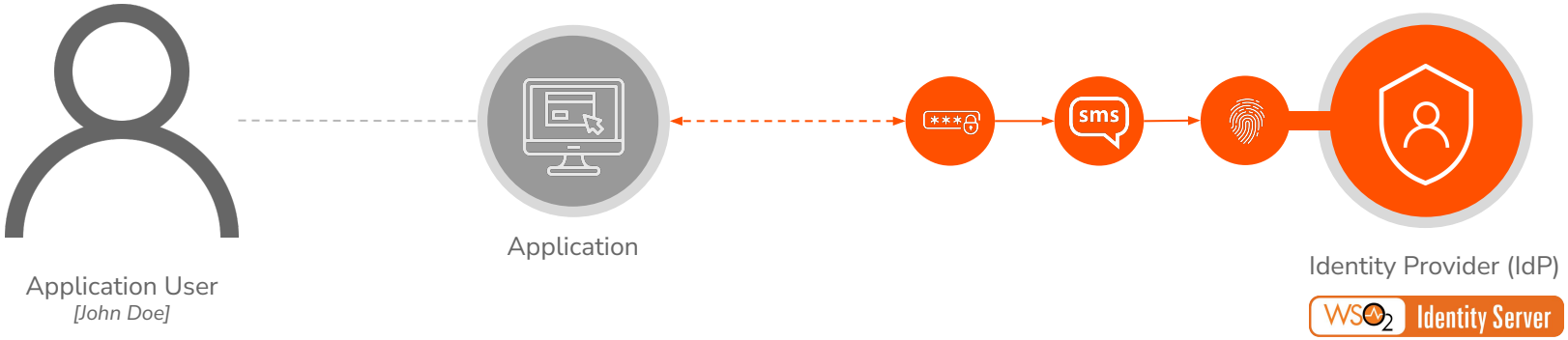
Single Sign-On (SSO)

Authenticate users once and allow access to other associated applications

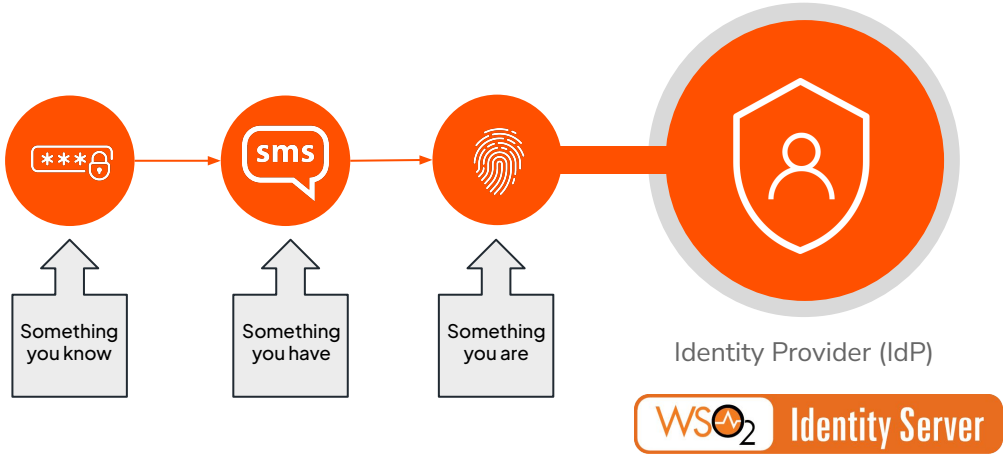


Multi-Factor Authentication (MFA)

Challenge users with multiple authentication factors such as password, SMS, and fingerprint

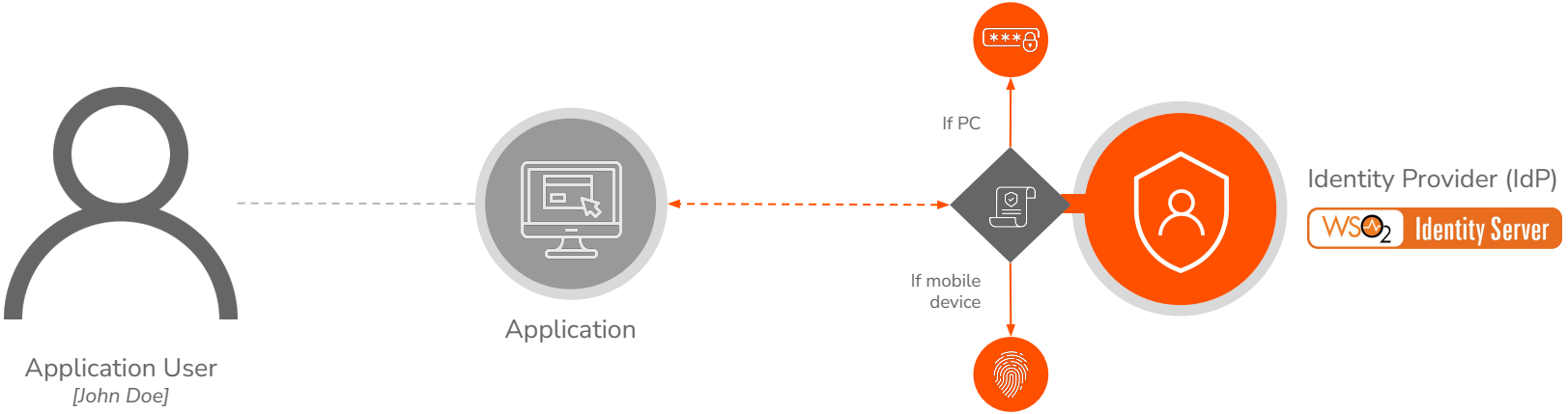


Multi-Factor Authentication (MFA)



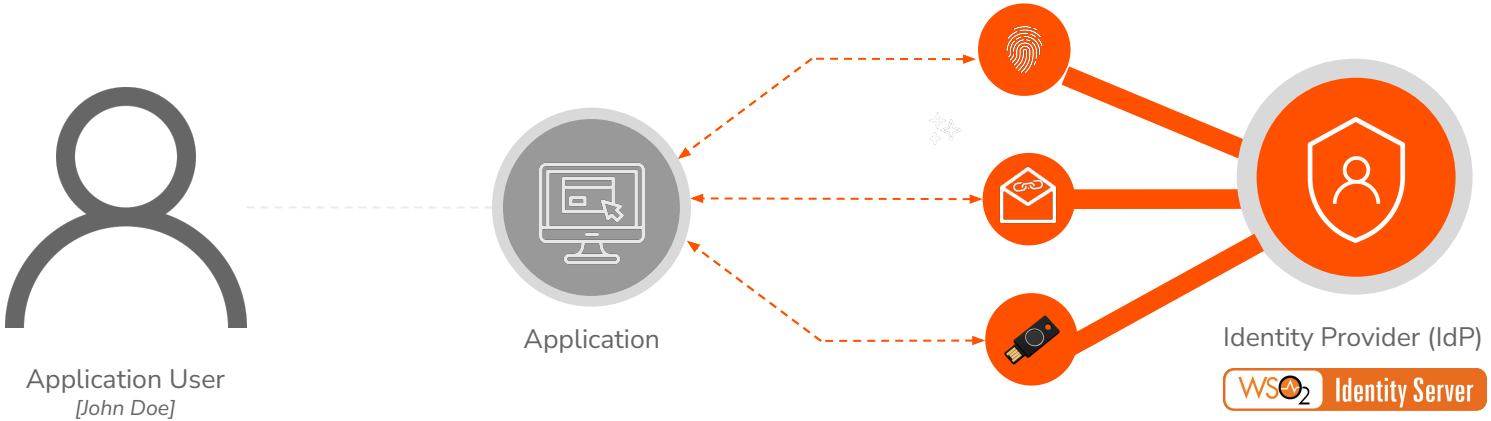
Adaptive Authentication

Challenge users with multiple authentication steps based on the users' risk profile



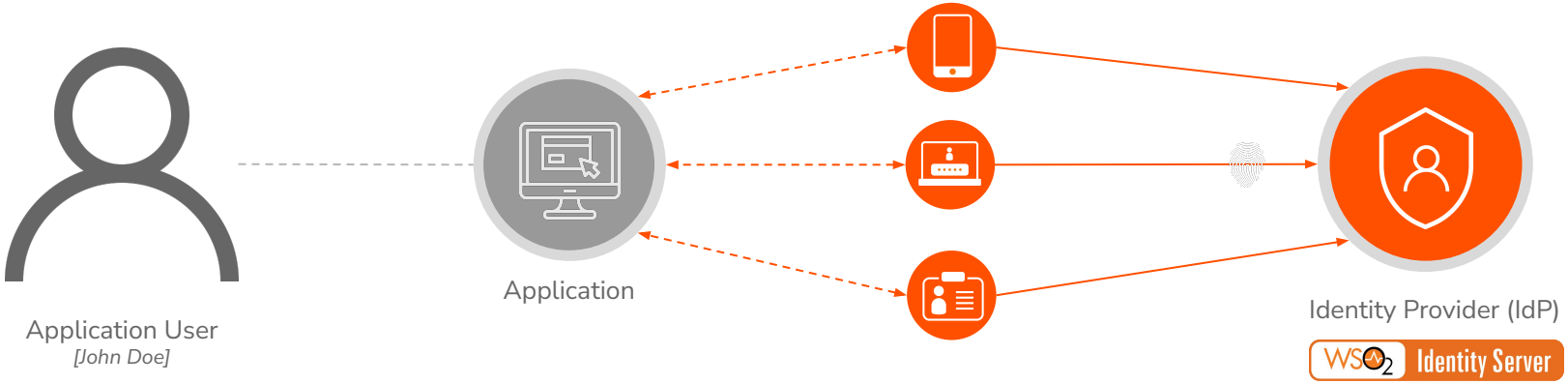
Passwordless Authentication

Authenticating users, using authentication mechanisms that does not use password such as magic link.



Multi-Attribute Login

Allow multiple attributes for identification during login such as mobile number, email, and employee ID .

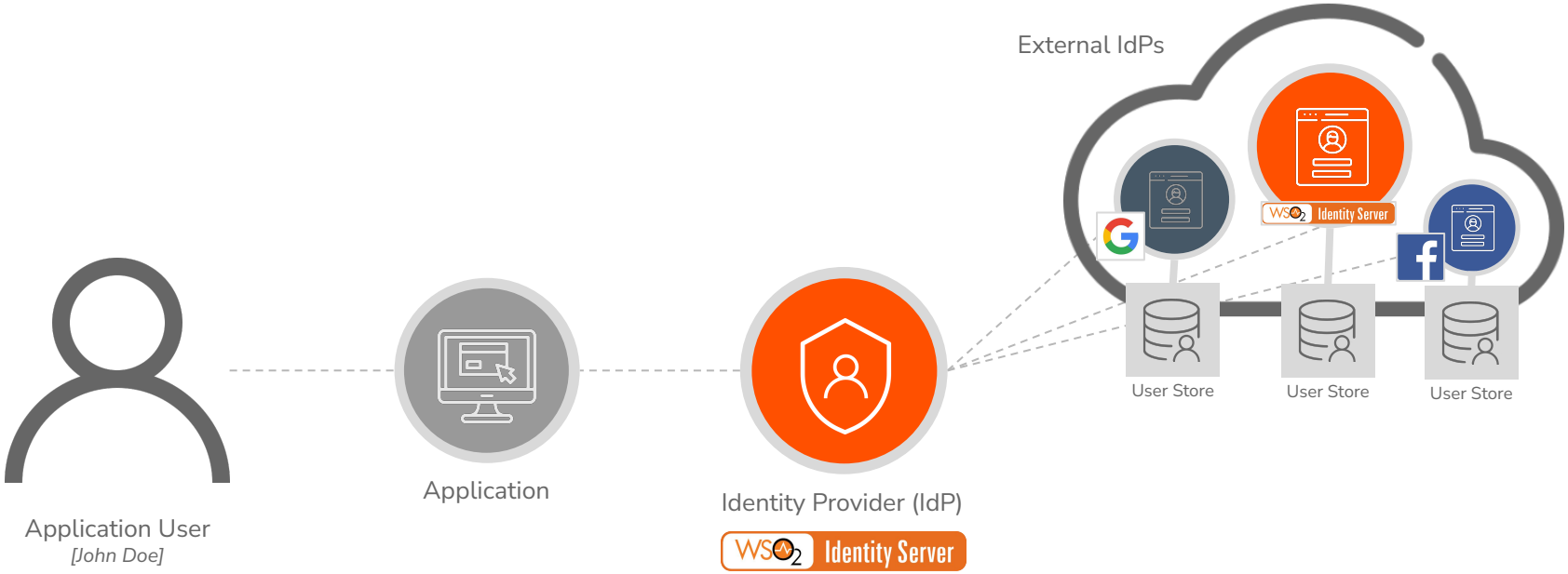


Identity Federation

Let users bring their identities from another identity provider

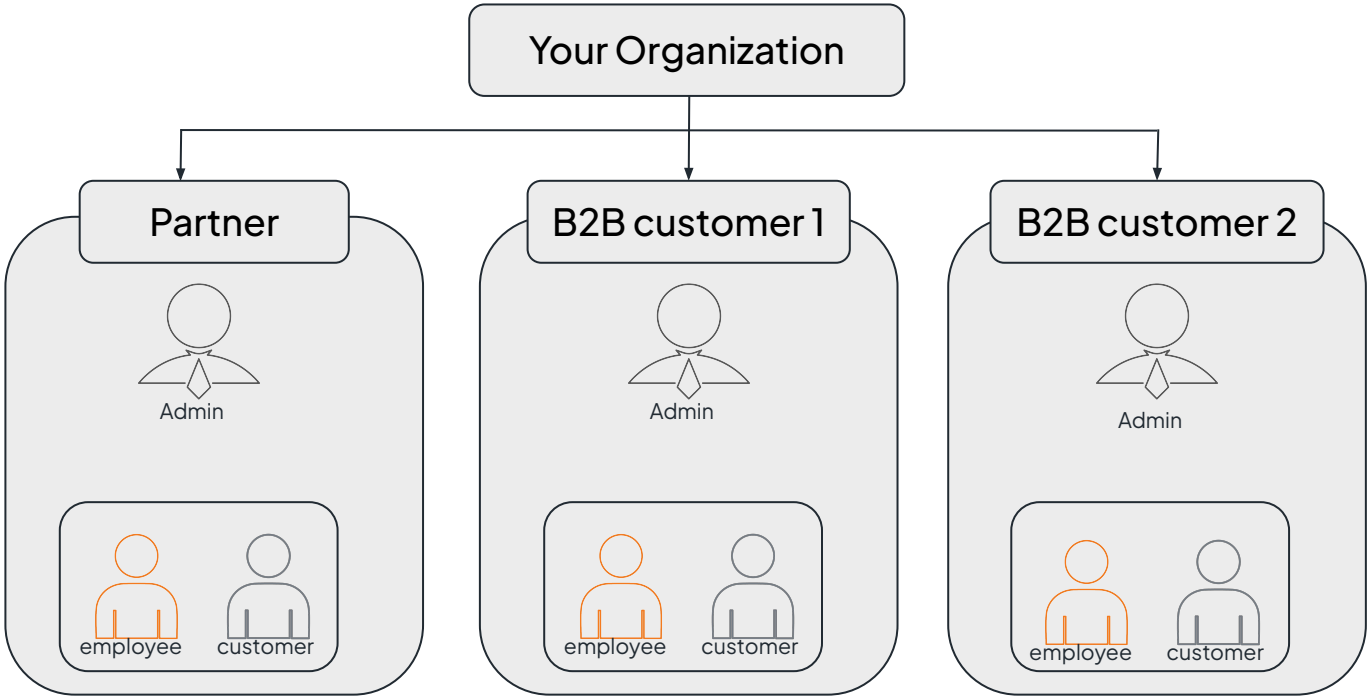
Identity Federation with Social Login

Let users bring their identities from a social service provider



Business-to-Business CIAM

Manage access to your organization for business customers / partners



Privacy and Regulatory Compliance

Identity Provider (IdP)

WSO2 Identity Server

WSO2 Identity Server

Value Proposition

- Fully open source (Apache 2.0 open source license)
- Multiple deployment options:
  - On-prem (WSO2 Identity Server)
  - Public SaaS (Asgardeo)
  - Private SaaS (IPK)
- Inherent extensibility for building a tailor-made IAM platform
- 24*7 support for production customers

Value Proposition

- 1+ billion identities managed worldwide
- 280+ direct subscription customers and 1200+ OEM-driven deployments
- Globally operating - main offices in USA, UK, Germany, Brazil, Australia, UAE, Malaysia and Sri Lanka

Industry Recognition

Overall leader and Product leader- KuppingerCole Leadership Compass on CIAM platforms - 2022/2020

Strong performer - The Forrester Wave™ on Customer Identity and Access Management - Q4 2022/2020

Leader overall - KuppingerCole Leadership Compass on Identity APIs - 2019

Product leader in LC: Access Management and Federation - 2018

Gartner Peer Insights - Rating 4.4(out of 5)

Key Features

- Web Single Sign-On (SSO) and Identity Federation
- Identity Bridging
- Adaptive and Strong - Multi Factor Authentication (MFA)
- Accounts Management and Identity Provisioning
- Branding and Internationalization
- API Access Management
- B2B CIAM
- Data privacy compliance
- Integration with CRM, Sales, and Marketing applications
- IAM developer tools

Key Benefits

- Avoids vendor lock-in with open source and open standards
- Extensible architecture allowing customization to support unique IAM use cases
- Accommodates large-scale deployments with millions of users
- Effortless integration with cloud and on-premises applications, third-party authentication systems, and social identity providers
- Hassle-free deployment and low-cost maintenance
- Flexibility to choose a preferred deployment: on-premise, public cloud, or private cloud.

Quick Recap

What you learnt

1. Traditional access management and its issues
2. An overview to IAM concepts and benefits
3. WSO2 Identity Server features and benefits

Any Questions ?

Reach us through the following channels

✉ iam-dev@wso2.org

https://stackoverflow.com/questions/tagged/wso2-identity-server

https://discord.com/invite/Xa5VubmThw

Thanks!

wso2.com